

CLAIMS

1-10 (Cancelled).

11. (Previously Presented) A method for ensuring that a processor will execute only authorized code, said method comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected;

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key; and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory upon verifying said digital signature.

12. (Cancelled)

13. (Previously Presented) A method as recited in claim 11 wherein the integrity of the contents of said protected memory is protected by encryption using a cryptographic key stored on said processor.

14. (Original) A method as recited in claim 11 wherein said protected memory is physically

protected.

15. (Cancelled)

16. (Original) A method as recited in claim 11 wherein the integrity of said authorized code is protected at run time.

17. (Original) A method as recited in claim 16 wherein the integrity of said authorized code is protected with symmetric key encryption.

18. (Original) A method as recited in claim 11 wherein the privacy of said authorized code is protected at run time.

19. (Original) A method as recited in claim 18 wherein the privacy of said authorized code is protected at run time with symmetric key encryption.

20-21. (Cancelled)

22. (Previously Presented) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform program steps for ensuring that a processor will execute only authorized code, the program steps comprising:

reading a certificate including a first public key into a protected memory;

validating said certificate with a second public key permanently stored on said processor;

reading a signed authorized code into said protected memory, wherein said protected memory is cryptographically protected;

preparing to execute said signed authorized code from the protected memory by verifying a digital signature used to sign said signed authorized code in accordance with said first public key; and

branching to a copy of said signed authorized code in said protected memory to begin execution and performing inline decryption of the copy of said signed authorized code in said protected memory upon verifying said digital signature.

23. (Previously Presented) A computing device for securely executing authorized code, said computing device comprising:

a protected memory for storing signed authorized code, which contains an original digital signature, wherein said protected memory is cryptographically protected; and

a processor in signal communication with said protected memory for preparing to execute said signed authorized code from the protected memory by verifying that a digital signature contained in said signed authorized code is original in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor, and if said original digital signature is verified, then branching to a copy of said authorized code in said protected memory to begin execution.

24. (Previously Presented) A computing device as recited in claim 23 wherein the integrity of the contents of said protected memory is protected by encryption.

25. (Previously Presented) A computing device as recited in claim 23 wherein said protected memory is physically protected.

26. (Previously Presented) A computing device as recited in claim 23 wherein at least one of the integrity of said authorized code and the privacy of said authorized code is protected at run time.

27. (Previously Presented) A computing device as recited in claim 23 wherein the integrity of said signed authorized code is protected at run time with symmetric key encryption.

28. (Previously Presented) A computing device as recited in claim 23, wherein the privacy of said signed authorized code is protected at run time with symmetric key encryption.